CLAIMS

1. A protocol for controlling access to information scrambled at a broadcast centre using a service key contained in a control word, the control word being encrypted by means of an operating key, the access control protocol consisting at least in sending said scrambled information and periodic access control messages, ECM messages, to at least one descrambling terminal associated with an access control module provided with a security processor, the ECM messages containing access criteria and the cryptogram of the control word, the control word and the cryptogram of the control word being changed periodically, access to said scrambled information at each descrambling terminal being conditional upon a "true" value for said access criteria when compared with at least one access right registered in the access control module, and then upon decrypting said cryptogram of the control word using the operating key, in order to recover said control word and to descramble said scrambled information,

the protocol being characterized in that it further consists:

· in assigning each access control message, ECM message, a number (T_j) satisfying a monotonic non-decreasing function, consecutive messages ECM_j with successive numbers representing a timebase formed by a plurality of individual time intervals for sending successive individual quanta of scrambled information;

· in detecting in each descrambling terminal the number (T_j) of each access control message, message ECM_j, and then, in response to a user request (UR) from the user of said descrambling terminal for conditional controlled access to at least a portion of said scrambled information;

· in selecting a number for an access control message, message ECM_j, the number corresponding to the

sending time of said request, and constituting a time origin (T_{jo}) of said timebase; and

as a function of a specific access criterion, in authorizing said user to access said scrambled information from said origin (T_{jo}) of said timebase over a time range corresponding to a plurality of individual time intervals defining a plurality of successive individual quanta of scrambled information.

2. A protocol according to claim 1, characterized in that said time range is defined by a first offset (td) from said origin (T_{jo}) corresponding to the beginning of the access as a function of said specific access criterion, and a second offset (tf) corresponding to the end of the access as a function of said specific access criterion.

3. A protocol according to claim 1 or claim 2, characterized in that said monotonic non-decreasing function is a continuously increasing function of the sending time of the control messages ECM_j.

4. A protocol according to claim 1 or claim 2, characterized in that said monotonic non-decreasing function is an increasing step function of the sending time of the control messages ECM_j.

5. A protocol according to claim 4, characterized in that each step is defined by a constant number over a plurality of sending times of the control messages ECM_j, which defines a timebase with a resolution different from the sending time of the control messages ECM_j.

6. A protocol according to claim 5, characterized in that each number is defined by a timestamp, each step being defined by the time range represented by two separate timestamps.

7. A protocol according to claim 2, characterized in that said specific access criterion corresponds to free access.

8. A protocol according to any one of claims 2 to 7, characterized in that said time range is either an interval backwards from said origin, $td \leq 0$ AND $tf \leq 0$, or an interval forwards from said origin, $td \geq 0$ AND $tf \geq 0$, or a forward and backward interval, $td \leq 0$ AND $tf \geq 0$.

9. A protocol according to any one of claims 1 to 8, characterized in that, in order to manage the number of viewings (NV) at the request of the user in accordance with said specific access criterion in said time range and outside said time range, the protocol consists at least:

· in defining a maximum authorized number of viewings (NVM);

· in testing whether the number of viewings (NV) is less than or equal to said authorized maximum number of viewings (NVM); and,

· in the event of a negative result of said test, refusing access to the scrambled information; else

· in testing whether said current number (T_j) is in said time range; and,

· in the event of said current number (T_j) being in said time range; in authorizing access to said scrambled information on the basis of the specific access criterion during said time range; else

· in authorizing access on the basis of a distinct access criterion other than specific access criterion and on condition that a Boolean variable representative of forward access authorization or of backward access authorization, respectively, presents a "true" value.

10. A protocol according to claim 9, characterized in

that it further consists:

· in defining a first Boolean variable (AV) whose "true" value is representative of authorization of forward access to said scrambled information beyond said time range, on the basis of an access criterion other than said specific access criterion; and

· in defining a second Boolean variable (AR) whose "true" value is representative of authorization of backward access to said scrambled information before said time range, on the basis of an access criterion other than said specific access criterion.

11. A protocol according to claim 9 or claim 10, characterized in that, if said current number (T_j) is not in said time range, said authorization of access based on an access criterion other than said specific access criterion and conditional upon the "true" value of said Boolean variables consists:

· in submitting said current number (T_j) and said first Boolean variable (AV) to a first logical test to verify whether said current number (T_j) is equal to or greater than said origin number (T_{jo}) and to verify whether said first Boolean value is "true" in order to authorize forward access to said scrambled information or to a second logical test to verify whether said current number (T_j) is equal to or the less than said origin number (T_{jo}) and to verify whether the value of said second Boolean variable is "true" in order to authorize backward access to said scrambled information and, in the event of a positive result of either of the first or second logical tests:

· in authorizing forward access, or backward access as the case may be to said scrambled information with no incrementing of the number of viewings and, in the event of a negative result of both the first and second logical tests:

· in testing whether said number of viewings (NV) is

less than the authorized maximum number of viewings (NVM); and

· in the event of a negative result of said test, in refusing access to the scrambled information and incrementing said number of viewings (NV) by 1, else

· in authorizing forward, respectively backward, access to said scrambled information.

12. A protocol according to claim 11, characterized in that, for a specific access control corresponding to a basic rewind service for a recording and an authorized maximum number of viewings NVM = 1, said time range is a backward range defined by td < 0 AND tf = 0, the first Boolean variable is "true", forward access being authorized, and the backward second Boolean variable is the complement of the "true" value, backward access not being authorized.

13. A protocol according to claim 11, characterized in that, for a specific access control corresponding to a free access preview service, said time range is a forward range defined by td = 0 AND tf > 0, the authorized maximum number of viewings is NVM = 1, the first and the second Boolean variables are "false", recording and/or backward access not being authorized.

14. A protocol according to claim 11, characterized in that, for looped transmission of scrambled information, said authorized maximum number of viewings is set at a particular value, said time range for access to the scrambled information has a specific value, the first Boolean variable is "true" and the second Boolean value is "false".